Federal Public Key Infrastructure
Technical Working Group
Meeting Minutes

Prepared for the General Services Administration
By SRA International

Friday
December 19, 2014

10:30 a.m. – 12:00 p.m.

Teleconference

Time	Topic	Presenter
10:30	Welcome & Opening Remarks	Ola Bello
10:35	Certificate Policy Change Request – EKU	Wendy Brown
10:40	Greatest Common Divisor / Collision Detection Presentation	Todd Johnson
12:00	Adjourn	Ola Bello

Attendance List

Note: If you have any additions/corrections to the attendance list please let us know. Some people may not have responded to the roll call, or may not have identified their organization.

Name	Organization
Baldridge, Tim	DoD
Bello, Ola	FPKIMA
Brown, Wendy	FPKIMA
Chokhani, Santosh	DoD
Cimmino, Giuseppe	FPKIMA
Donohue, Paul	OMB
Foradori, Keith	DEA
Hansen, Maryam	DoD
Johnson, Todd	Treasury
Jung, Jimmy	State
Liston, Matthew	Treasury
McBride, Terry	Treasury
Myers, Kenneth	FPKIMA
Robinson, Buddy	Treasury
Salgado, John	DoD
Shorter, Scott	Electrosoft
Sulser, David	NRC
Wallace, Carl	DoD
Wyatt, Terry	NASA

Agenda Item 1 - Welcome and Opening remarks (Ola Bello)

The FPKI TWG met via teleconference to discuss a potential new certificate threat. Mr. Kenneth Myers introduced the new chair of the TWG, Mr. Ola Bello. Mr. Bello thanked everyone for calling in today and looks forward to working with the TWG members in the future. Mr. Bello then turned it over to Wendy Brown to discuss the next agenda item.

Agenda 2 – Certificate Policy Change Request EKU (Wendy Brown)

Ms. Brown briefly described the two change requests presented in the Certificate Policy Working Group (CPWG).

1. The first change proposal is a modification to the *Federal Public Key Infrastructure (FPKI) X.509 Certificate and CRL Extensions Profile [FPKI-Prof]*. This change request makes the use of anyEKU optional when EKU is asserted in the Key Management certificate to mitigate a potential risk in code signing certificates.
2. The second change proposal is a modification to the *FPKI X.509 Certificate and CRL Extensions Profile for PIV-I*. This change request makes the use of anyEKU optional when EKU is asserted in PIV-I Authentication and PIV-I Digital Signature certificates.

Ms. Brown explained the TWG previously discussed making the EKU extension mandatory in all end-entity certificates and prohibiting the inclusion of the anyEKU value, but was unable to reach consensus. These change proposals are a compromise position that allows issuing CAs to include the EKU without asserting anyEKU which essentially allows the certificate to be used for any purpose, intended or not. CPWG is requesting the TWG review the requests and provide comments to the CPWG.

There was a question whether a similar change proposal was being proposed for PIV. The answer is there could be, again the change would only be to the *X.509 Certificate and CRL Extentions Profile for the Shared Service Provider Program*, as EKU is not mentioned in the Certificate Policy itself.

The change proposals were not reviewed in detail during the meeting.

Agenda 3 – Greatest Common Divisor / Collision Detection (Todd Johnson)

Mr. Todd Johnson introduced the agenda item by explaining there has been extensive work in academia and the commercial space around detecting certificate anomalies and the TWG should integrate the work being done to increase the security of the FPKI. The presentation will cover two topics:

1. **Batch Greatest Common Divisor (GCD)** – This method divides certificate public key by a list of known GCDs to determine if the random number generator

(RNG) is flawed. If the result of computation has a weak RNG then the output may show non-random sequences for further investigation.

2. **Digest Collisions** – This is another method to detect anomalies and is most prevalent with MD5 and SHA-1 certificate keys. The greatest benefit for this method is to detect malicious forgeries such as in digitally signed documents.

Microsoft has a Certificate Reputation (CertRep) program through the Internet Explorer "SmartScreen" program which tests web browser and code signing certificates. Some academic papers on this topic include:

- "Ron was Wrong, Whit is Right"
- "Mining your Ps and Qs: Detection of Widespread Weak Keys in Network Devices"
- "Factoring RSA keys from Certified Smart Cards: Coppersmith in the Wild"

A number of questions were asked about practical application in the FPKI and a few suggestions were made for potential actions which include:

1. Contact Microsoft to present the CertRep program to the TWG
2. Contact CA operators and vendors about their efforts in GCD or Collision Detection to analyze current and future certificates for weak RNG anomalies

Agenda Item 4 - Wrap-up and Adjourn Meeting (Ola Bello)

Suggestions were made for topics for future meetings:

- Mr. Johnson requested Mr. Tim Baldridge give his Smartcard Alliance presentation on the CAC WMATA pilot.
- Presentation on the Treasury SCVP service, possibly include other vendor SCVP demonstrations and any Agency requirements for SCVP
- Possible follow-up discussion on GCD analysis:
    1. How do we securely share information about weaknesses found?
    2. How do we ensure commercial entities doing this type of analysis will share discovered information with the FPKI?

Mr. Bello thanked those in attendance and closed the meeting as it had run twenty minutes over.